

# SUPPLIER MANAGEMENT SYSTEM has a file upload (RCE) vulnerability

There is a file upload (RCE) vulnerability in the SUPPLIER MANAGEMENT SYSTEM. The vulnerability exists in the `btn_functions.php` file, which can upload any file format and execute any code to access the server.

## Supplier Or Admin Information

Id	Email	First Name Last Name		Mobile no	User Type	User Role	Picture	Action
8	admin@gmail.com	sami	Al Gaffer	1921078484	Admin	Active		<a href="#">Edit</a> <a href="#">Delete</a>
9	sami@gmail.com	nabil	nabil	4324	Supplier	Active		<a href="#">Edit</a> <a href="#">Delete</a>
10	s@gmail.com	samia	dsf	234	Supplier	Active		<a href="#">Edit</a> <a href="#">Delete</a>

## Update Supplier Or Admin

Email :

s@gmail.com

Password :

•

First Name :

samia


Last Name :

dsf

Mobile :

234

Gender : ☒ Male ☐ Female

Date of Birth: yyyy/mm/日 

Address:




















fsdfdsf

Choose Picture : [选择文件](#) 未选择文件

User Type: ☐ Admin ☒ Supplier

User Role: ☒ Active ☐ Inactive

▼ images

-  american-express....
-  bird.jpg
-  cropper.jpg
-  img.png
-  img2.jpg
-  img3.jpg
-  inbox.png
-  mastercard.png
-  media.jpg
-  paypal.png
-  picture.jpg
-  prod-1.jpg
-  prod-2.jpg
-  prod-3.jpg
-  prod-4.jpg
-  prod-5.jpg
-  test.php
-  user.png
-  visa.png



## PHP Version 5.4.45



System	Windows NT DESKTOP-M4LV1AG 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)